

Unlocking the Cloud Operating Model

Achieving the fastest path to value
in a modern, hybrid-cloud datacenter



Executive Summary

To thrive in an era of hybrid-cloud architecture, driven by digital transformation, Enterprise IT must evolve from ITIL-based gatekeeping to enabling shared self-service processes for DevOps excellence.

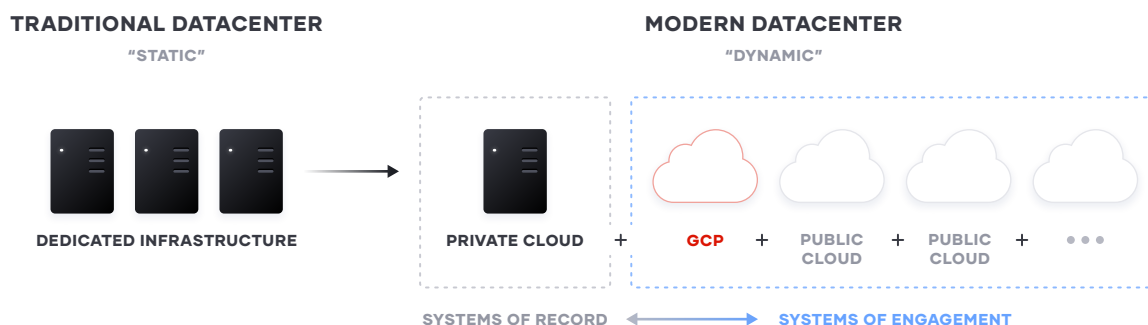
For most enterprises, digital transformation efforts mean delivering new business and customer value more quickly, and at a very large scale. The implication for Enterprise IT then is a shift from cost optimization to speed optimization. The cloud is an inevitable part of this shift as it presents the opportunity to rapidly deploy on-demand services with limitless scale.

To unlock the fastest path to value of the cloud, enterprises must consider how to industrialize the application delivery process across each layer of the cloud, embracing the cloud operating model, and tuning people, process, and tools to it.

In this white paper, we look at the implications of the cloud operating model, and present solutions for IT teams to adopt this model across infrastructure, security, networking, and application delivery.

Transitioning to a Hybrid-Cloud Datacenter

The transition to cloud and hybrid-cloud environments is a generational transition for IT. This transition means shifting from largely dedicated servers in a private datacenter to a pool of compute, network, and storage capacity – available on demand. While many enterprises began with one cloud provider, there are good reasons to use services from others. Inevitably most Global 2000 organizations will use more than one, either by design, regulatory compliance, or through mergers and acquisitions.

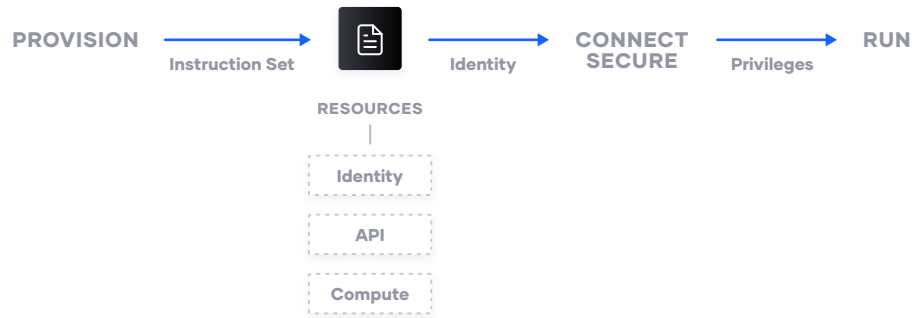


The cloud presents an opportunity for speed and scale optimization for new systems of engagement – the applications built to engage customers. These new apps are the primary interface for the customer to engage with a business, government agency, or non-profit organization, and are ideally suited for delivery in the cloud as they tend to:

- Have dynamic usage characteristics, needing to scale loads up and down by orders of magnitude during short time periods
- Be under pressure to quickly build and iterate. Many of these new systems may be ephemeral in nature, delivering a specific user experience around an event or campaign

For most enterprises, these systems of engagement must connect to existing systems of record – the core business databases and internal applications, which often continue to reside on infrastructure in existing data centers. As a result, enterprises end up with a hybrid setup – a mix of multiple public and private cloud environments.

In addition, the underlying primitives have changed from manipulating virtual machines (VMs) in a self-contained environment, to manipulating cloud resources in a shared environment. Enterprises then have the challenge of maintaining their existing estate, while developing the new cloud infrastructure.











The era of cloud computing has continued to decompose the units of management in infrastructure toward fine grained resources. A resource is essentially a unit of compute fit for some purpose that has an API and identity.

For cloud computing to work, there needs to be consistent workflows that can be reused at scale across multiple cloud providers. Hence these resources require:

- Consistent instruction sets for provisioning
- Identity for security and for network connections
- Privileges and rights so they can be deployed and run

Implications of the Cloud Operating Model

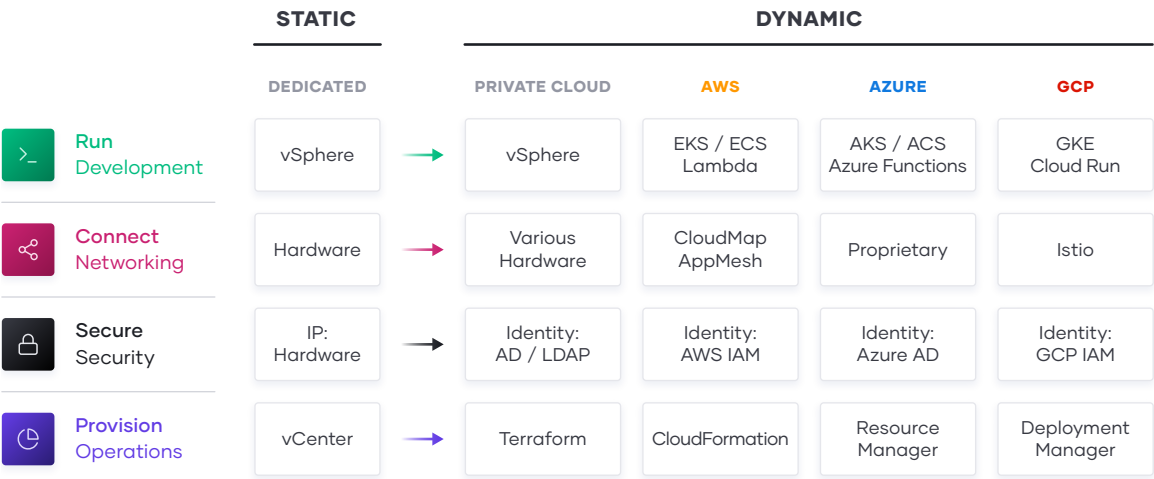
The essential implication of the transition to the cloud is the shift from “static” infrastructure to “dynamic” infrastructure from a focus on configuration, and management of a static fleet of IT resources, to provisioning, securing, connecting, and running dynamic resources on demand.

	STATIC		DYNAMIC
 Run	Dedicated Infrastructure		Scheduled across the fleet
 Connect	Host-based Static IP		Service-based Dynamic IP
 Secure	High trust IP-based		Low trust Identity-based
 Provision	Dedicated servers Homogeneous		Capacity on-demand Heterogeneous

Decomposing this implication, and working up the stack, various changes of approach are implied:

- **Provision.** The infrastructure layer transitions from running dedicated servers at limited scale to a dynamic environment where organizations can easily adjust to increased demand by spinning up thousands of servers and scaling them down when not in use. As architectures and services become more distributed, the sheer volume of compute nodes increases significantly.
- **Secure.** The security layer transitions from a fundamentally “high-trust” world enforced by a strong perimeter and firewall to a “low-trust” or “zero-trust” environment with no clear or static perimeter. As a result, the foundational assumption for security shifts from being IP-based to using identity-based access to resources.
- **Connect.** The networking layer transitions from being heavily dependent on the physical location and IP address of services and applications to using a dynamic registry of services for discovery, segmentation, and composition. An enterprise IT team does not have the same control over the network, or the physical locations of compute resources, and must think about service-based connectivity.
- **Run.** The runtime layer shifts from deploying artifacts to a static application server to deploying applications with a scheduler atop a pool of infrastructure which is provisioned on-demand. In addition, new applications have become collections of services that are dynamically provisioned, and packaged in multiple ways: from virtual machines to containers.

Additionally, each cloud provider has its own solution to these challenges. For enterprise IT teams, these shifts in approach are compounded by the realities of running on hybrid- and hybrid-cloud infrastructures and the varying tools each technology provides.



To address these challenges those teams must ask the following questions:

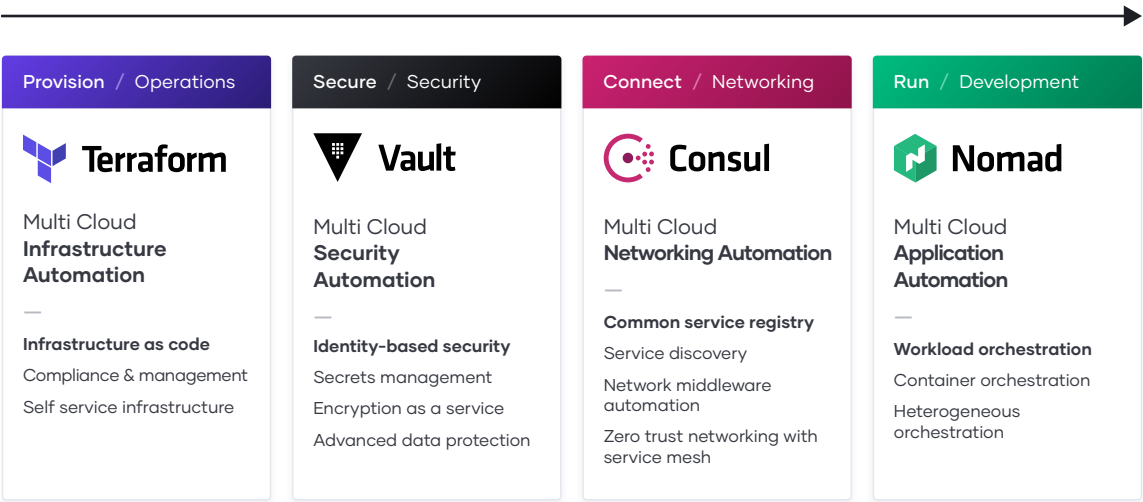
- **People.** How can we enable a team for a hybrid-cloud reality, where skills can be applied consistently regardless of target environment?
- **Process.** How do we position central IT services as a self-service enabler of speed, versus a ticket-based gatekeeper of control, while retaining compliance and governance?
- **Tools.** How do we best unlock the value of the available capabilities of the cloud providers in pursuit of better customer and business value?

Unlocking the Cloud Operating Model on Google

As the implications of the cloud operating model impact teams across infrastructure, security, networking, and applications, we see a repeating pattern amongst enterprises of establishing central shared services with centers of excellence to deliver the dynamic infrastructure necessary at each layer for successful application delivery.

As teams deliver on each shared service for the cloud operating model, IT velocity increases. The greater cloud maturity an organization has, the faster its velocity.

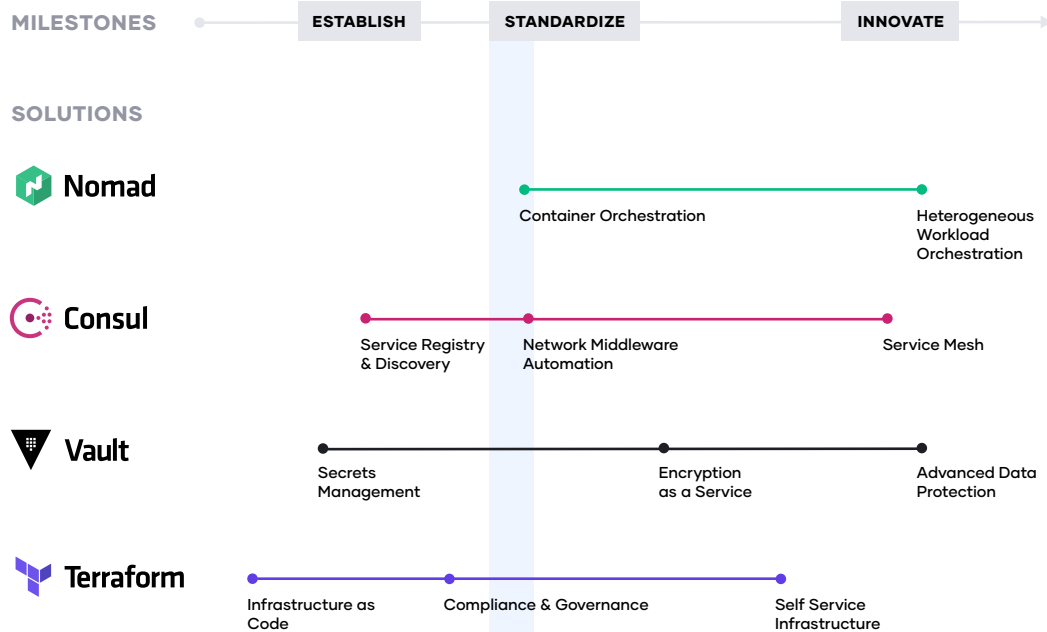
EXPANDING USE OF THE HASHICORP STACK INCREASES MATURITY AND VELOCITY FOR OUR CUSTOMERS



The typical journey we have seen customers adopt, as they unlock the cloud operating model, involves three major milestones:

- 1. Establish the cloud essentials** – As you begin your journey to the cloud, the immediate requirements are provisioning the cloud infrastructure typically by adopting infrastructure as code and ensuring it is secure with a secrets management solution. These are the bare necessities that will allow you to build a scalable and truly dynamic cloud architecture that is futureproof.
- 2. Standardize on a set of shared services** – As cloud consumption starts to pick up, you will need to implement and standardize on a set of shared services so as to take full advantage of what the cloud has to offer. This also introduces challenges around governance and compliance as the need for setting access control rules and tracking requirements become increasingly important.

3. **Innovate using a common logical architecture** – As you fully embrace the cloud and depend on cloud services and applications as the primary systems of engagement, there will be a need to create a common logical architecture. This requires a control plane that connects with the extended ecosystem of cloud solutions and inherently provides advanced security and orchestration across services and multiple clouds.

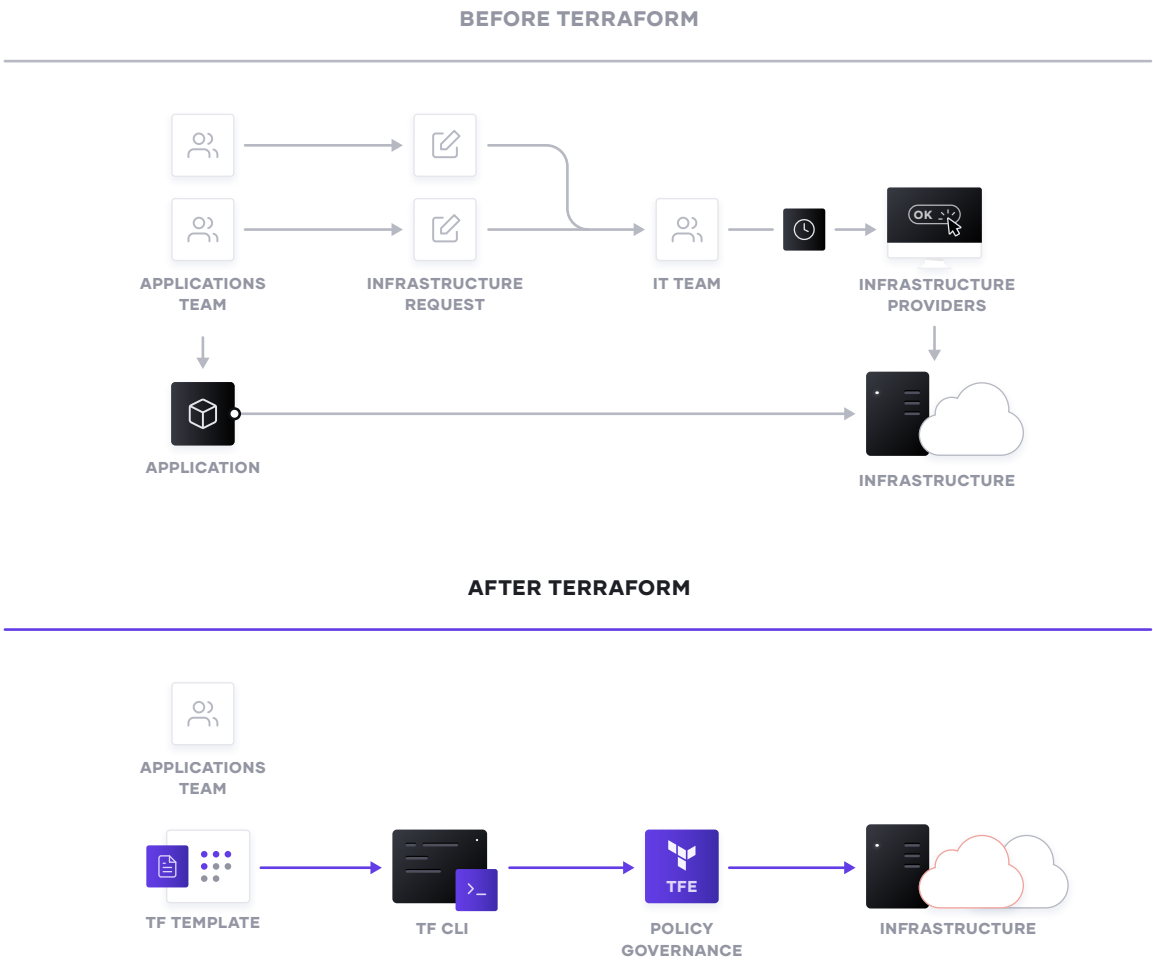


What follows is the step-by-step journey that we have seen organizations adopt successfully.

Step 1: Hybrid-Cloud Infrastructure Provisioning

The foundation for adopting the cloud is infrastructure provisioning. HashiCorp Terraform is used to provision infrastructure for any application using an array of providers for any target platform.

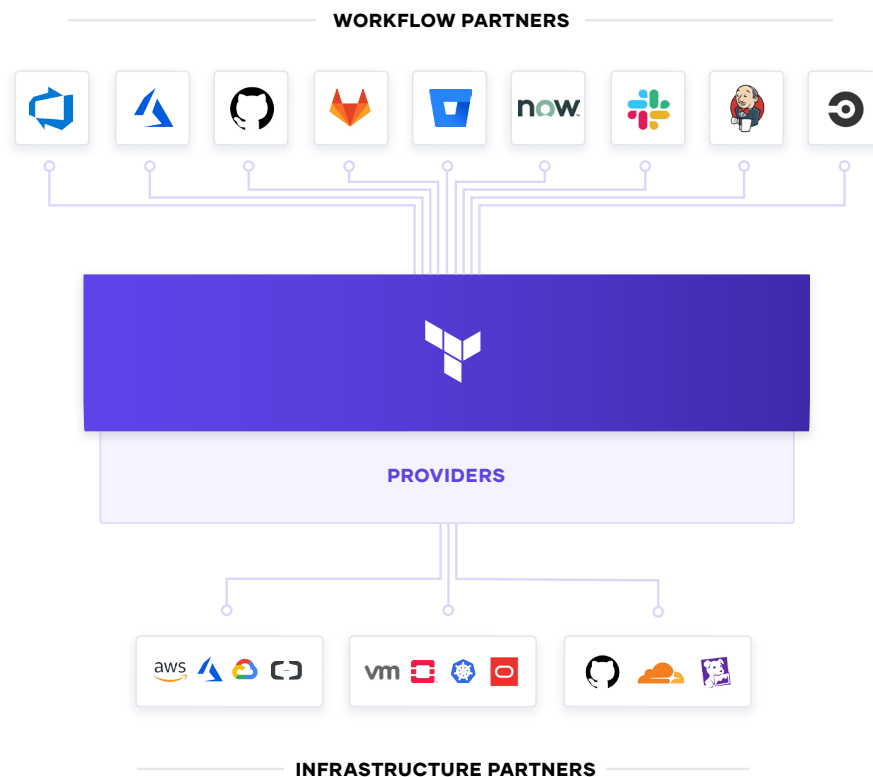
To achieve shared services for infrastructure provisioning, IT teams should start by implementing reproducible infrastructure as code practices, and then layering compliance and governance workflows to ensure appropriate controls.



Reproducible Infrastructure as Code

The first goal of a shared service for infrastructure provisioning is to enable the delivery of reproducible infrastructure as code, providing teams a way to plan and provision resources inside CI/CD workflows using familiar tools throughout.

Teams can create Terraform templates that express the configuration of services from one or more cloud platforms. Terraform integrates with most major configuration management tools to allow fine grained provisioning to be handled following the provisioning of the underlying resources. Finally, templates can be extended with services from many other ISV providers to include monitoring agents, application performance monitoring (APM) systems, security tooling, DNS, and CDNs, and more. Once defined, the templates can be provisioned as required in an automated way. In doing so, Terraform becomes the adopted language and common workflow for teams provisioning resources across public and private cloud.



For self-service IT, the decoupling of the template-creation process and the provisioning process greatly reduces the time taken for any application to go live since developers no longer need to wait for operations approval, as long as they use a pre-approved template.

Compliance and Management

For most teams, there is also a need to enforce policies on the type of infrastructure created, how it is used, and which teams get to use it. HashiCorp's Sentinel policy as code framework provides compliance and governance without requiring a shift in the overall team workflow, and is defined as code too, enabling collaboration and comprehension for DevSecOps.

Without policy as code, organizations often resort to using a ticket-based review process to approve changes. This results in developers waiting weeks or longer to provision infrastructure and becomes a bottleneck. Policy as code allows teams to solve this by splitting the definition of the policy from the execution of the policy.

Centralized teams codify policies enforcing security, compliance, and operational best practices across all cloud provisioning. Automated enforcement of policies ensures changes are in compliance without creating a manual review bottleneck.

Step 2: Hybrid-Cloud Security

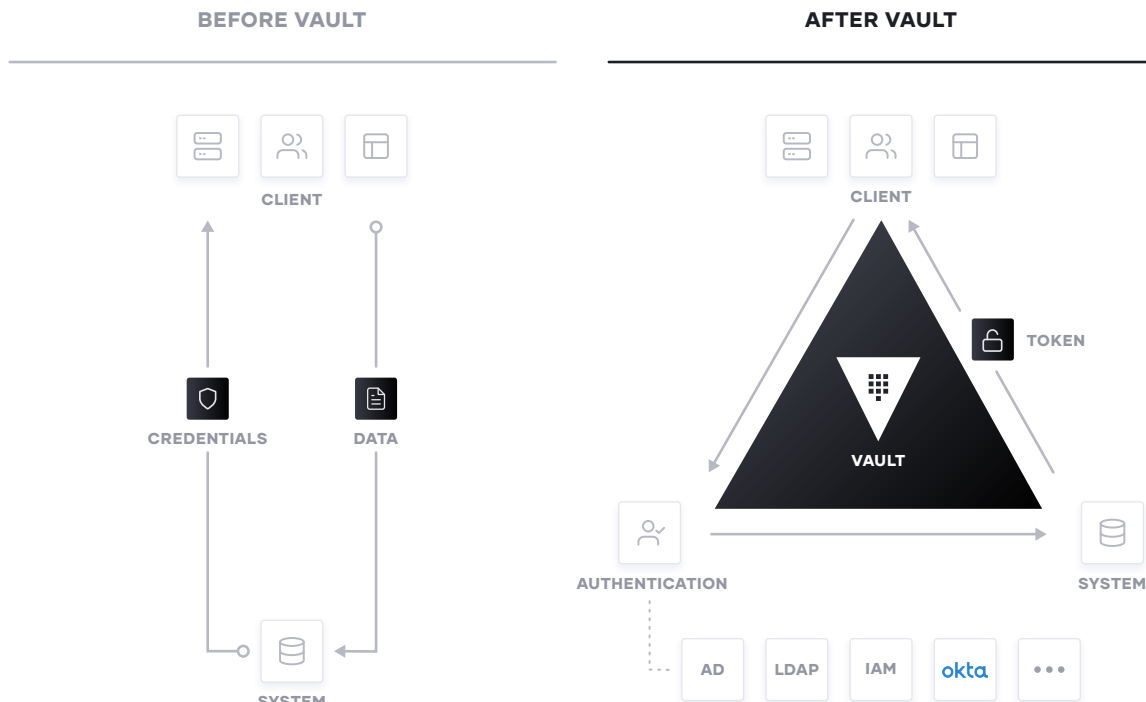
Dynamic cloud infrastructure means a shift from host-based identity to application-based identity, with low or zero-trust networks across multiple clouds without a clear network perimeter.

In the traditional security world, we assumed high trust internal networks, which resulted in a hard shell and soft interior. With the modern “zero trust” approach, we work to harden the inside as well. This requires that applications be explicitly authenticated, authorized to fetch secrets and perform sensitive operations, and tightly audited.

HashiCorp Vault enables teams to securely store and tightly control access to tokens, passwords, certificates, and encryption keys for protecting machines and applications. Vault helps protect data at rest and data in transit. Vault exposes a high level API for cryptography for developers to secure sensitive data without exposing encryption keys. Vault also can act like a certificate authority, to provide dynamic short lived certificates to secure communications with SSL/TLS. Lastly, Vault enables a brokering of identity between different platforms, such as Active Directory on premises and Google Cloud IAM to allow applications to work across platform boundaries.

Vault is widely used across stock exchanges, large financial organizations, hotel chains, and everything in between to provide security in the cloud operating model.

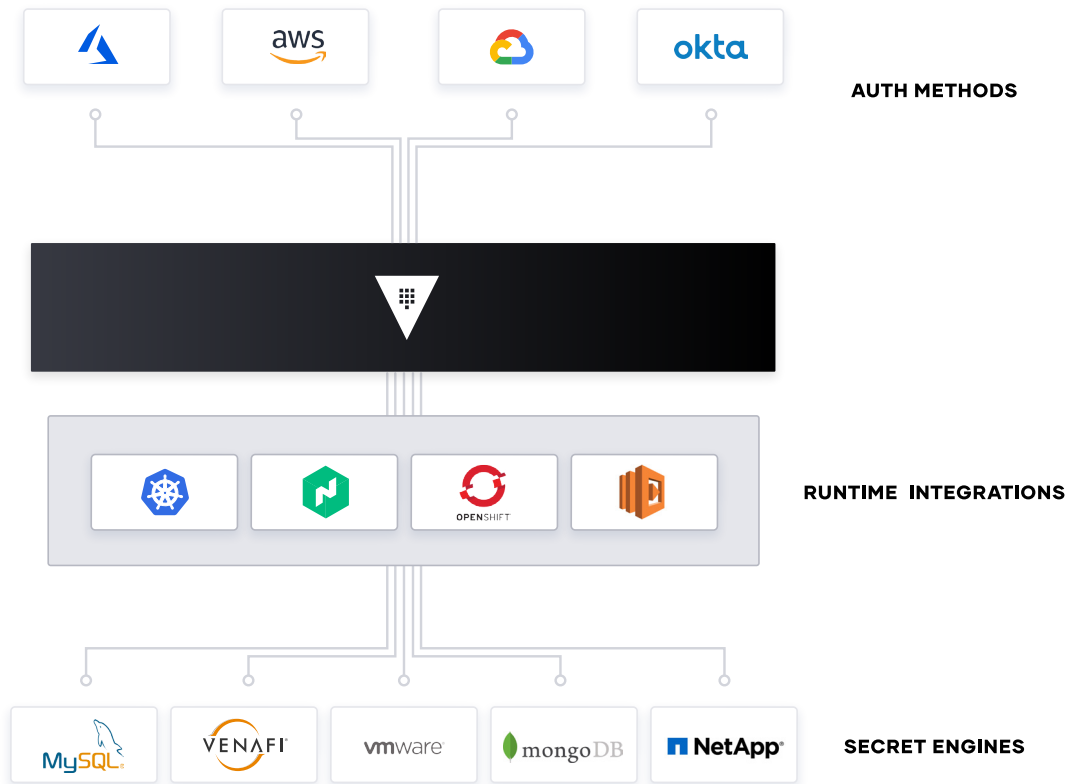
To achieve shared services for security, IT teams should enable centralized secrets management services, and then use that service to deliver more sophisticated encryption-as-a-service use cases such as certificate and key rotations, and encryption of data in transit and at rest.



Secrets Management

The first step in cloud security is typically secrets management: the central storage, access control, and distribution of dynamic secrets. Instead of depending on static IP addresses, integrating with identity-based access systems such as Google Cloud IAM to authenticate and access services and resources is crucial.

Vault uses policies to codify how applications authenticate, which credentials they are authorized to use, and how auditing should be performed. It can integrate with an array of trusted identity providers such as cloud identity and access management (IAM) platforms, Kubernetes, Active Directory, and other SAML-based systems for authentication. Vault then centrally manages and enforces access to secrets and systems based on trusted sources of application and user identity.



Enterprise IT teams should build a shared service which enables the request of secrets for any system through a consistent, audited, and secured workflow.

Encryption as a Service

Additionally, enterprises need to encrypt application data at rest and in transit. Vault can provide encryption-as-a-service to provide a consistent API for key management and cryptography. This allows developers to perform a single integration and then protect data across multiple environments.

Using Vault as a basis for encryption-as-a-service solves difficult problems faced by security teams such as certificate and key rotation. Vault enables centralized key management to simplify encrypting data in transit and at rest across clouds and datacenters. This helps reduce costs around expensive Hardware Security Modules (HSM) and increases productivity with consistent security workflows and cryptographic standards across the organization.

While many organizations provide a mandate for developers to encrypt data, they don't often provide the "how" which leaves developers to build custom solutions without an adequate understanding of cryptography. Vault provides developers a simple API that can be easily used, while giving central security teams the policy controls and lifecycle management APIs they need.

Advanced Data Protection

Organizations moving to the cloud or spanning hybrid environments still maintain and support on-premise services and applications that need to perform cryptographic operations, such as data encryption for storage at rest. These services do not necessarily want to implement the logic around managing these cryptographic keys, and thus seek to delegate the task of key management to external providers. Advanced Data Protection allows organizations to securely connect, control, and integrate advanced encryption keys, operations, and management between infrastructure and Vault Enterprise, including automatically protecting data in MySQL, MongoDB, PostgreSQL, and other databases using transparent data encryption (TDE).

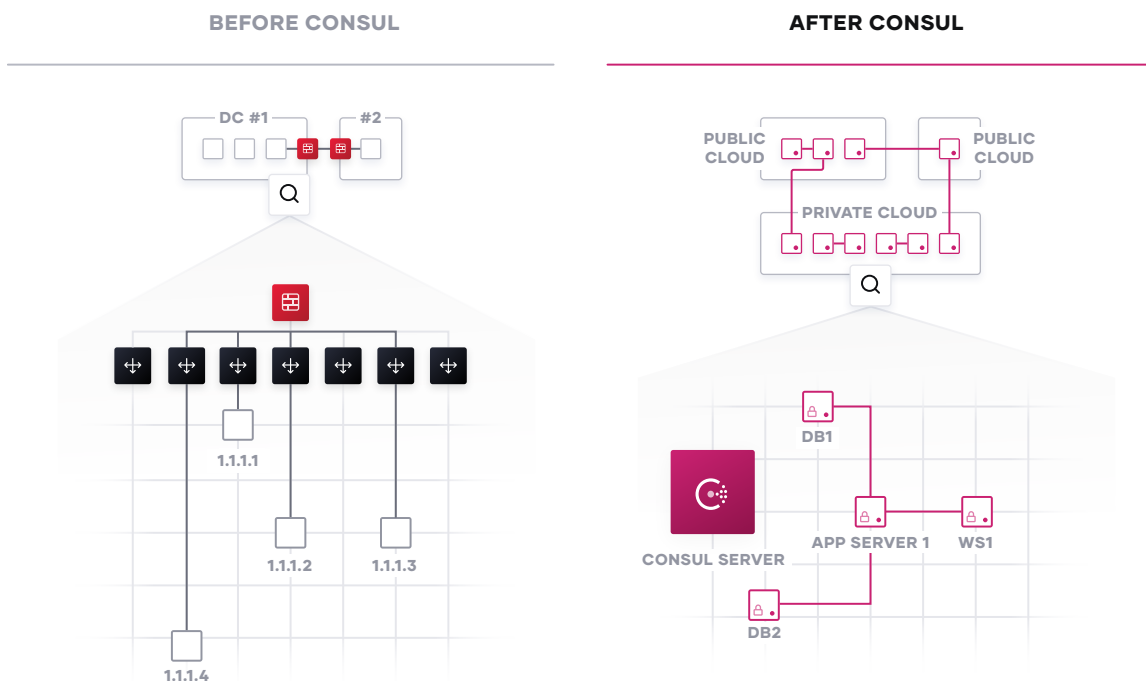
For organizations that have high security requirements for data compliance (PCIDSS, HIPAA, etc), protecting data, and cryptographically-protecting anonymity for personally identifiable information (or PII), Advanced Data Protection provides organizations with functionality for data tokenization, such as data masking, to protect sensitive data, such as credit cards, sensitive personal information, bank numbers, etc.

Step 3: Hybrid-Cloud Service Networking

The challenges of networking in the cloud are often one of the most difficult aspects of adopting the cloud operating model for enterprises. The combination of dynamic IP addresses, a significant growth in east-west traffic as the microservices pattern is adopted, and the lack of a clear network perimeter is a formidable challenge.

HashiCorp Consul provides a hybrid-cloud service networking layer to connect and secure services. Consul is a widely deployed product, with many customers running significantly greater than 100,000 nodes in their environments.

Networking services should be provided centrally, whereby IT teams provide service registry and service discovery capabilities. Having a common registry provides a “map” of what services are running, where they are, and their current health status. The registry can be queried programmatically to enable service discovery or drive network automation of API gateways, load balancers, firewalls, and other critical middleware components. These middleware components can be moved out of the network by using a service mesh approach, where proxies run on the edge to provide equivalent functionality. Service mesh approaches allow the network topology to be simplified, especially for hybrid-cloud and multi-datacenter topologies.



Service Discovery

The starting point for networking in the cloud operating model is typically a common service registry, which provides a real-time directory of what services are running, where they are, and their current health status. Traditional approaches to networking rely on load balancers and virtual IPs to provide a naming abstraction to represent a service with a static IP. The process to track the network location of services often takes the form of spreadsheets, load balancer dashboards, or configuration files, all of which are disjointed, manual processes that are not ideal.

For Consul, each service is programmatically registered and DNS and API interfaces are provided to enable any service to be discovered by other services. The integrated health check will monitor each service instance's health status so the IT team can triage the availability of each instance and Consul can help prevent routing traffic to unhealthy service instances.

Consul can be integrated with other services that manage existing north-south traffic such as traditional load balancers, and distributed application platforms such as Kubernetes, to provide a consistent registry and discovery service across multi-datacenter, cloud, and platform environments.

Network Middleware Automation

The next step is to reduce operational complexity with existing networking middleware through network automation. Instead of a manual, ticket-based process to reconfigure load balancers and firewalls every time there is a change in service network locations or configurations, Consul can automate these network operations. This is achieved by enabling network middleware devices to subscribe to service changes from the service registry, enabling highly dynamic infrastructure that can scale significantly higher than static-based approaches.

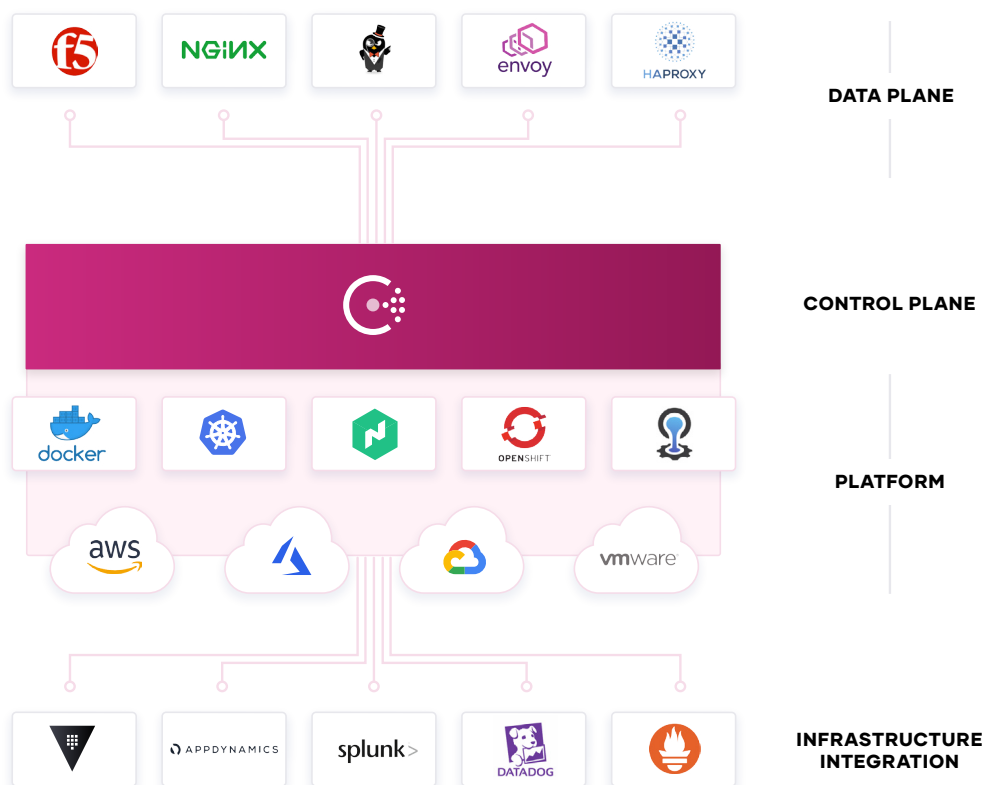
This decouples the workflow between teams, as operators can independently deploy applications and publish to Consul, while NetOps teams can subscribe to Consul to handle the downstream automation.

Zero Trust Networking with Service Mesh

As organizations continue to scale with microservices-based or cloud-native applications, the underlying infrastructure becomes larger and more dynamic with an explosion of east-west traffic. This causes a proliferation of expensive network middleware with single points of failure and significant operational overhead exposed to IT teams.

Consul provides a distributed service mesh that pushes routing, authorization, and other networking functionalities to the endpoints in the network, rather than imposing them through middleware. This makes the network topology simpler and easier to manage, removes the need for expensive middleware within east-west traffic paths, and it makes service-to-service communication much more reliable and scalable.

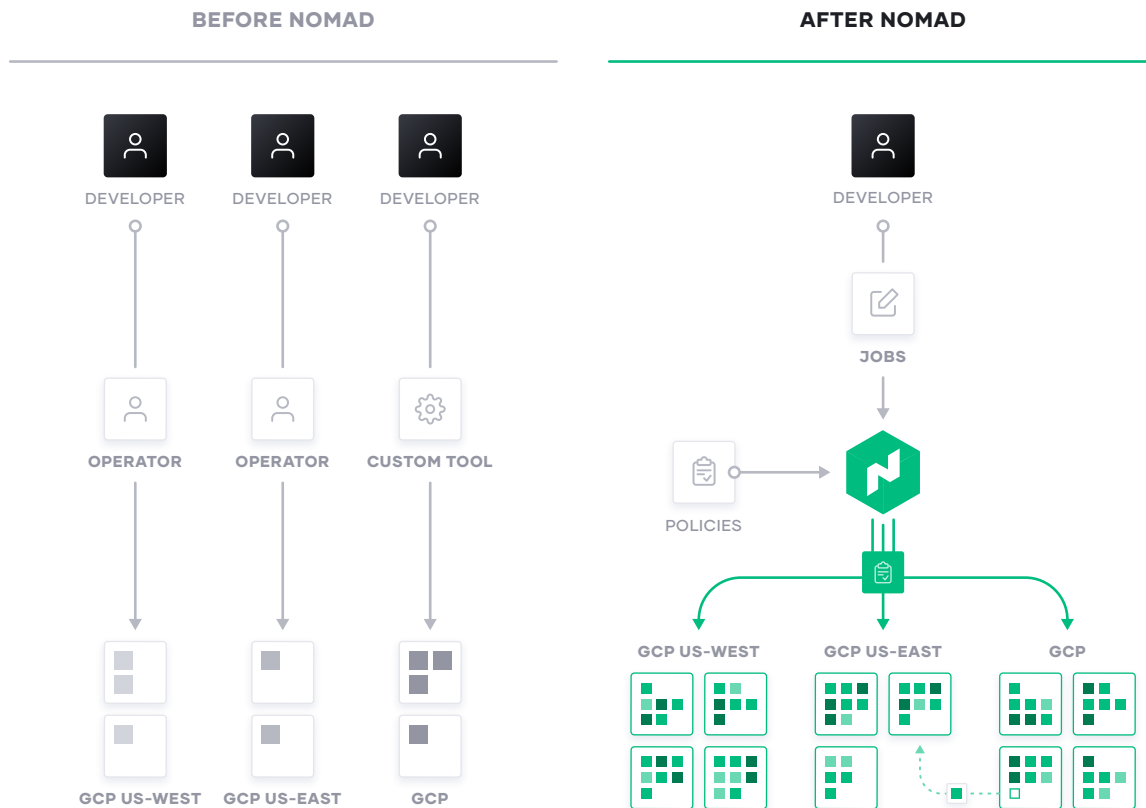
Consul is an API-driven control plane that integrates with sidecar proxies alongside each service instance (proxies such as Envoy, HAProxy, and NGINX). These proxies provide the distributed data plane. Together, these two planes enable a zero trust network model that secures service-to-service communication with automatic TLS encryption and identity-based authorization. Network operation and security teams can define the security policies through intentions with logical services rather than IP addresses.



Step 4: Hybrid-Cloud Application Delivery

Finally, at the application layer, new apps are increasingly distributed while legacy apps also need to be managed more flexibly. HashiCorp Nomad provides a flexible orchestrator to deploy and manage legacy and modern applications, for all types of workloads: from long running services, to short lived batch, to system agents.

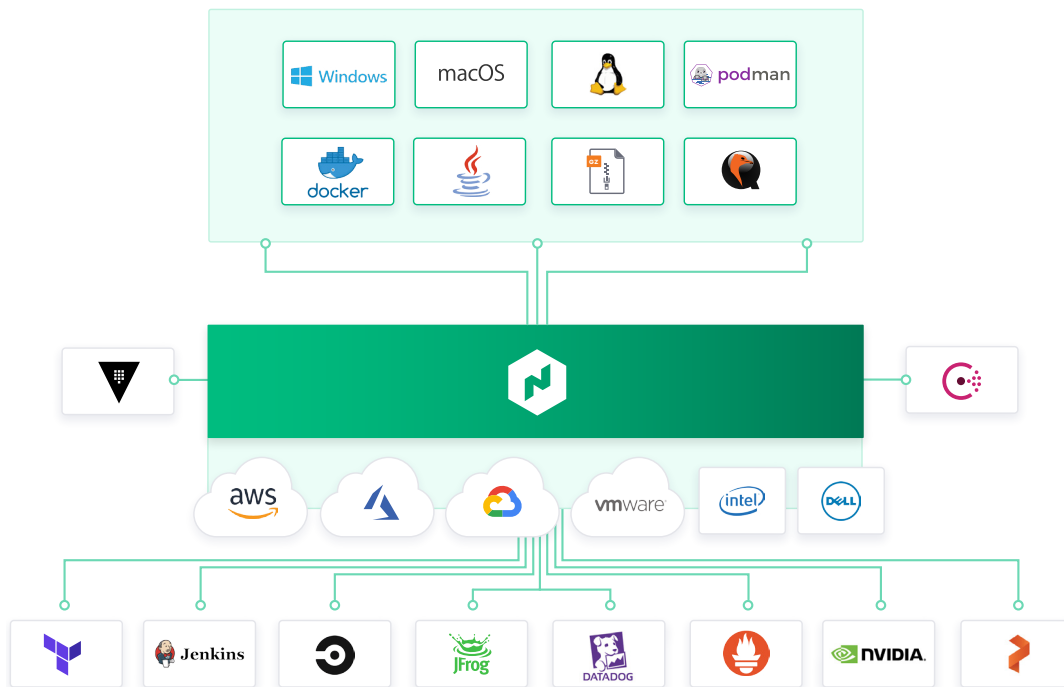
To achieve shared services for application delivery, IT teams should use Nomad in concert with Terraform, Vault, and Consul to enable the consistent delivery of applications on cloud infrastructure, incorporating necessary compliance, security, and networking requirements, as well as workload orchestration and scheduling.



Mixed Workload Orchestration

Many new workloads are developed with container packaging with the intent to deploy to Kubernetes or other container management platforms. But many legacy workloads will not be moved onto those platforms, nor will future Serverless applications. Nomad provides a consistent process for deployment of all workloads from virtual machines, through standalone binaries, and containers, and provides core orchestration benefits across those workloads such as release automation, multiple upgrade strategies, bin packing, and resilience.

For modern applications with built-in containers, Nomad provides the same consistent workflow at scale in any environment. Nomad is focused on simplicity and effectiveness at orchestration and scheduling, and avoids the complexity of platforms such as Kubernetes that require specialist skills to operate and solve only for container workloads.



Nomad integrates into existing CI/CD workflows to provide fast, automatic application deployments for legacy and modern workloads.

High Performance Compute

Nomad is designed to schedule applications with low latency across very large clusters. This is critical for customers with large batch jobs, as is common with High Performance Computing (HPC) workloads. In the million container challenge, Nomad was able to schedule one million instances of Redis across 5,000 machines in three data centers, in under 5 minutes. Several large Nomad deployments run at even larger scales.

Nomad enables high performance applications to easily use an API to consume capacity dynamically, enabling efficient sharing of resources for data analytics applications like Apache Spark. The low latency scheduling ensures results are available in a timely manner and minimizes wasted idle resources.

Multi-Datacenter Workload Orchestration

Nomad is multi-region and hybrid-cloud by design, with a consistent workflow to deploy any workload. As teams roll out global applications in multiple data centers, or across cloud boundaries, Nomad provides orchestrating and scheduling for those applications, supported by the infrastructure, security, and networking resources and policies to ensure the application is successfully deployed.

Conclusion

A common cloud operating model is an inevitable shift for enterprises aiming to maximize their digital transformation efforts. The HashiCorp suite of tools seeks to provide solutions for each layer of the cloud to enable enterprises to make this shift to the cloud operating model.

Enterprise IT needs to evolve away from ITIL-based control points with its focus on cost optimization, toward becoming self-service enablers focused on speed optimization. It can do this by delivering shared services across each layer of the cloud designed to assist teams deliver new business and customer value at speed.

Unlocking the fastest path to value in a modern multi-cloud data center through adopting a common cloud operating model means shifting characteristics of Enterprise IT:

- **People: Shifting to multi-cloud skills**
 - Reuse skills from internal data center management and single cloud vendors and apply them consistently in any environment.
 - Embrace DevSecOps and other agile practices to continuously deliver increasingly ephemeral and distributed systems.
- **Process: Shifting to self-service IT**
 - Position Central IT as an enabling shared service focused on application delivery velocity: shipping software every more rapidly with minimal risk.
 - Establish centers of excellence across each layer of the cloud for self-service delivery of capabilities.
- **Tools: Shifting to dynamic environments**
 - Use tools that support the increasing ephemerality and distribution of infrastructure and applications and that support the critical workflows rather than being tied to specific technologies.
 - Provide policy and governance tooling to match the speed of delivery with compliance to manage risk in a self-service environment.

About HashiCorp

HashiCorp is the leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp open source tools Vagrant, Packer, Terraform, Vault, Consul, and Nomad are downloaded tens of millions of times each year and are broadly adopted by the Global 2000. Enterprise versions of these products enhance the open source tools with features that promote collaboration, operations, governance, and multi-data center functionality. The company is headquartered in San Francisco and backed by Mayfield, GGV Capital, Redpoint Ventures, True Ventures, IVP, and Bessemer Venture Partners. For more information, visit www.hashicorp.com or follow HashiCorp on Twitter [@HashiCorp](https://twitter.com/HashiCorp).

